# Sophisticated Spy Kit Targets Russians with Rare GSM Plugin

By Tara Seals

Published: 2019-10-10 · Archived: 2026-04-05 21:41:31 UTC

The Attor malware targets government and diplomatic victims with unusual tactics.

A sophisticated cyberespionage platform called Attor has come to light, sporting an unusual capability for fingerprinting mobile devices as part of its attacks on government and diplomatic victims.

According to researchers at ESET, Attor, which has flown under the radar since at least 2013, also sports a complex modular architecture and elaborate network communications utilizing Tor, making it a highly evolved threat.



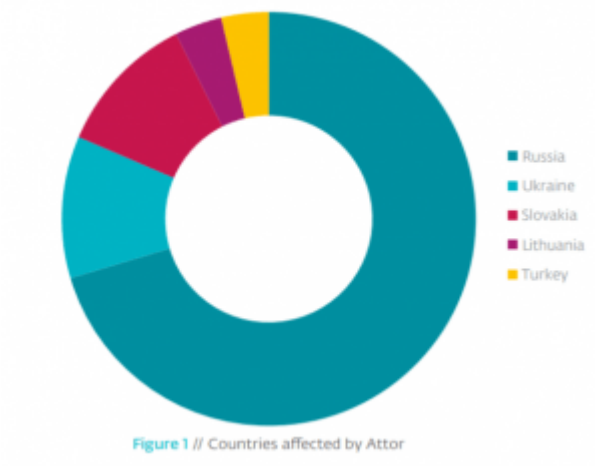


Figure 1 // Countries affected by Attor

Click to enlarge.

The malware, researchers said, has been used in espionage campaigns as recently as this summer; however, the offensives are highly targeted, with only a few dozen victims recorded. Attor appears to go after Russian-based, Russian-speaking users, based on geographic telemetry as well as the fact that it was seen snooping on Russian applications; this includes taking screenshots of Russian instant messenger (IM) apps.

ESET noted that some targets are located in Eastern Europe.

## GSM Plugin

As far as its architecture goes, Attor hinges on a dispatcher, which serves as a management and synchronization unit; all of Attor's capabilities are provided as plugins. This allows the attackers to customize the platform on a per-victim basis, researchers said.

One of Attor's most notable modules is a GSM fingerprinting tool that ESET noted utilizes a rarely used AT command set (it's this combined with "Tor" that gives the malware its name). AT commands, also known as Hayes command set, were originally developed in the 1980s to command a modem to dial, hang up or change connection settings. The command set was subsequently extended, and now supports other phone devices, including mobile devices.

"The commands are still in use in most modern smartphones," ESET researchers said in a posting on Thursday. "[It's possible] to bypass security mechanisms and communicate with the smartphones using AT commands through their USB interface. [In research], thousands of commands were recovered and tested, including those to send SMS messages, push touch events, or leak sensitive information. This … illustrates that the old-school AT commands pose a serious risk when misused."

As for Attor's plugin, ESET said that it seems unlikely it is targeting modern smartphone devices; it ignores devices connected via a USB port, and only contacts those connected to a network via a serial COM port.

"A more likely explanation of the plugin's main motive is that it targets modems and older phones," according to the research. "Alternatively, it may be used to communicate with some specific devices (used by the victim or target organization) that are connected to the COM port or to the USB port using a USB-to-serial adaptor. In this scenario, it is possible the attackers have learned about the victim's use of these devices using some other reconnaissance techniques."

Regardless, the plugin retrieves the name of manufacturer, model number, IMEI number and software version for the mobile phone or GSM/GPRS modem, along with information on the subscriber's carrier.

ESET noted that these fingerprints are likely used to tailor the deployment of additional commands to the specific devices.

| AT command | Functionality |
|---|---|
| AT | Signals start of communication (AT for attention). |
| AT+MODE=2 | Prepares the phone for an extended AT+ command set. |
| AT+CGSN | Requests IMEI number (International Mobile Equipment Identity), which is a unique number to identify a device. |
| AT+CGMM | Requests information about the model of the device (model number). |
| AT+CGMI | Requests name of the device manufacturer. |
| AT+CGMR | Requests the version of the software loaded on the device. |
| AT+CNUM | Requests MSISDN (Mobile Station International Subscriber Directory Number), which is the mapping of the telephone number to the subscriber identity module in a mobile or cellular phone. |
| AT+CIMI | Requests IMSI (International Mobile Subscriber Identity), which is a unique number identifying a GSM subscriber. This number has two parts. The initial part is comprised of six digits in the North American standard and five digits in the European standard. It identifies the GSM network operator in a specific country with whom the subscriber holds an account. The second part is allocated by the network operator to uniquely identify the subscriber. |

Aside from the GSM module, other Attor plugins provide persistence, an exfiltration channel to upload files, command-and-control (C2) communication and several further spying capabilities such as audio recording

capabilities.

One of the plugins is a screengrabber, which takes screenshots of social networks, email services, office software, archiving utilities, cloud storage and file sharing services, and VoIP applications and messaging services. Also targeted are applications that suggest that the attackers are specifically interested in privacy-conscious users, including TrueCrypt and other encryption/digital signature utilities, a VPN application (HMA VPN), secure mail clients (The Bat! and HushMail) and a secure web browser (Dragon).

## Use of Tor and Malware Timeline

Attor also incorporates Tor to avoid tracking, and distributes network communications to help thwart analysis.

“Plugins themselves are heavily synchronized, with network communication alone being spread across four different components, each implementing a different layer,” explained researchers. “This allows the malware to communicate with its FTP C&C server, which resides on an onion domain. Tor is used for communication, aiming for anonymity and untraceability, and the overall setup makes it impossible to analyze the communication unless all pieces of the puzzle have been collected.”

That’s one of the reasons that ESET wasn’t able to uncover the full operation timeline, nor how the malware initially entered the victim organizations. The analysis did show that Attor has been active in two waves: One in 2013 (only detected this year); and another that began in 2018 and continued through July.

Nonetheless, the campaign – and the actors behind it – bear watching, the firm warned: “We were not able to recover the full operation timeline, nor the initial access vector. The versioning information in the plugins suggests there are other plugins that we have not yet seen. However, our research provides a deep insight into the malware, and suggests that it is well worth further tracking of the operations of the group behind this malware.”

***What are the top cyber security issues associated with privileged account access and credential governance? Experts from Thycotic will discuss during our upcoming free Threatpost webinar, “Hackers and Security Pros: Where They Agree & Disagree When It Comes to Your Privileged Access Security.” Click here to register.***

---